DOD Privacy Impact Assessment (PIA)

1. DA organizational name (APMS Sub Organization name).

U. S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System (APMS System name).

Headquarters, Army Civilian Personnel System (HQ ACPERS) Reports.

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR).

605

5. IT Investment (OMB Circular A11) Unique Identifier (if applicable).

N/A

6. Privacy Act system of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and expiration date.

N/A

8. Type of Authority to collect information (statutory or otherwise):

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532 and 5533;
5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 3013, Secretary of the Army;
Executive Order 9397;
Army Regulation 690-200;
Army Regulations 215-1 and 215-3

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup).

The purpose of the HQ ACPERS system is to provide a modern, common, automated operating infrastructure in support of the Army Civilian Personnel community in the accomplishment of its assigned mission. The application's main function is to collect, collate and produce reports regarding civilian personnel supporting the Department of the Army. HQ ACPERS is an existing system that is in the operation/support life cycle phase. The system contains information pertaining to Army civilian workforce personnel.

HQ ACPERS is a data repository that is organized into three subsystems to facilitate administration, resource organization, maintenance, operation, and support. The subsystems are update subsystem, reporting subsystem, and query subsystem. The data repository consists of an Oracle database, plus backup and history files. The system is connected to the Department of Defense (DoD) Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) via the installation backbone. HQ ACPERS interfaces through a secure network for inputs and outputs. Data inputs are provided by the Defense Civilian Personnel Data System (DCPDS), Corporate Management Information System (CMIS), National Guard data repository, Office of Personnel Management (OPM), and the Customer Service Unit (CSU). Outputs are of three types. The first type consists of standard formatted reports that do not contain Privacy Act protected data, which are posted on the Civilian Personnel Online (CPOL) website. Army users access CPOL through the NIPRNET through the use of a Web browser. The second output type consists of data extract files that contain privacy act protected data, which are posted on a Sensitive but Unclassified (SBU) server with restricted access via a secure network to specific personnel on a need-to-know basis. The third output type consists of interfaces via a secure network with using information systems to include Business Objects Army (BOA) and the Civilian Productivity Report (CivPro) system. Web servers, application servers, and database servers are located within Army Civilian Data Center (ACDC) located at Rock Island, Illinois.

Full database backups are run weekly. System event logs are checked weekly by the administrator / information assurance security officer (IASO). Tapes are stored at an offsite commercial facility in Atlanta, Georgia.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Information in identifiable form that will be collected includes: Name, username, social security number (SSN), date of birth, age, gender, citizenship, race, ethnicity, dependent status, marital status, address, region, agency, command, pay plan, pay grade, prior pay grade, salary, prior salary, hazardous duty pay type, foreign language pay level and amount, recruitment pay, supervisory status, work schedule, duty location, army functional designator, educational level, academic institution name, college major or minor, credit hours, degree(s) attained and date(s), career program position, clearance status, veterans status, occupational code, unit id code, personnel office id, Equal Employment Opportunity (EEO) data, health plan benefits information, retirement plan benefits information, award history, award amounts, appraisal history, position type and history, employment status and nationality.

11. Describe how the information will be collected.

Information used by HQ ACPERS is extracted daily, on occurrence or monthly from DCPDS, CMIS, and the National Guard repository, OPM, and CSU via a secure network connection.

12. Describe the requirement and why the information in identifiable form is to be collected.

The purpose of the HQ ACPERS system is to provide a modern, common, automated operating infrastructure to manage and oversee Army Civilian Personnel functions. The Office of the Assistant Chief of Staff for Civilian Personnel was established under the Secretary of the Army to carry out these mandates. Information in identifiable form is collected and used by this system in direct support of this mission.

13. Describe how the information in identifiable form will be used (e.g., to verify data, etc.).

The information will be formatted into standardized report or data structures on various civilian manpower and functional reports which are distributed to government agencies, departments within the Army, and authorized personnel with whom a documented System Interface Agreement exists.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The system does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within and outside Department of the Army.

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Internal DoD agencies that would obtain access to Personally Identifiable Information (PII) in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense

Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Defense Manpower Data Center, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form.

Information used by HQ ACPERS is extracted daily, on occurrence and monthly from DCPDS, CMIS, and the National Guard repository, OPM, and CSU via a secure network connection. Individuals are not involved in this process. Individuals are implicitly consenting to the capture and use of this information when employed by the Department of Army civilian workforce where they are initially provided a Privacy advisory.

17. Describe any information that is provided to and individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Information in identifiable form is not collected directly from the individual thus they are not provided a Privacy Act Statement or Privacy Advisory.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentially of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Cameras are also used to monitor activity around the installation. System users include Army Civilian Personnelists and administrative/technical support personnel assigned to the HQ ACPERS. Personnelists do not process classified information and are not required to have a DoD security clearance. Personnel with system administration privileges are required to have background investigations at the automatic data processing / information technology (ADP/IT) I or II level and to sign a non-disclosure statement. All personnel accessing government computer information are required to have a minimum of ADP/IT III background investigation.

Users, both government and contractor, may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role.

Each specific application in the system may further restrict access via application-unique permission controls. Users must enter appropriate user Identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is routine monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system of collection of information will require a System of Records Notice (SORN). If not published, state when publication of the notice will occur.

The system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risks the collection, use, and sharing of the information in identifiable form.

Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data. Accordingly, due to the level of safeguarding, we believe that the risk to individuals' privacy is minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale.

The data in the system is For Official Use Only. The PIA may be published in full.